

RECEIVED  
CENTRAL FAX CENTER

JAN 16 2007

## SECTION II—REMARKS

Applicants thank the Examiner for a thorough review, and respectfully request reconsideration of the above referenced patent application for the following reasons:

**Allowable Subject Matter**

Applicants acknowledge that claims 5-6, 11-12, 15-16, 20-21, 27-28, and 31-32 were objected to as being dependent upon rejected base claims, but would be allowable if rewritten in independent form.

**Claims 5, 11, 15, 20, 27, and 31**

Claims 5, 11, 15, 20, 27, and 31 are canceled herein without prejudice, thus rendering their allowable status moot. Applicants have incorporated the limitations of said claims into the amended independent claims presented herein.

**Claims 6, 12, 16, 21, 28, and 32**

Applicants respectfully assert that the rejection of the independent claims from which claims 6, 12, 16, 21, 28, and 32 depend is overcome as set forth in Applicants remarks herein with reference to the § 103(a) rejection below. Accordingly, Applicants respectfully submit that said claims are in condition for allowance as presented or amended herein.

**Claims 1-3, 7-9, 13, 18, 23-25, and 29 rejected under 35 U.S.C. § 103(a)**

Claims 1-3, 7-9, 13, 18, 23-25, and 29 were rejected under 35 U.S.C. § 103(a) as being

unpatentable over US patent 6,189,098 to Kaliski, Jr. ("Kaliski"), and in further view of US 6,886,0995 to Hind, et al. ("Hind").

Claim 1 as amended herein recites the following:

A method performed by a user terminal of a wireless access network, the method comprising:

**scrambling a user terminal certificate using a first portion of a shared secret to be known only by the user terminal and an access point of the wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;**

**disqualifying the first portion of the shared secret from use with symmetric key cryptography between the user terminal and the access point;**

**generating an authenticator string including data encrypted with the user terminal private key; and**

**sending a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.**

Support for this added limitation may be found in original claim 5, and paragraph [0028] of the specification. Independent claims 7 and 23 recite similar limitations of "scrambling a user terminal certificate using a first portion of a shared secret ... [and] **disqualifying the first portion of the shared secret from use with symmetric key cryptography between the user terminal and the access point.**" Independent claims 13, 18, and 29 likewise recite similar claims, but "**unscramble** the user terminal certificate" instead of "scramble." Claim 13 specifically recites "**unscrambling the user terminal certificate using a first portion of the decrypted shared secret ... [and] disqualifying the first portion of the decrypted shared secret from use with symmetric key cryptography between the user terminal and the access point.**"

Kaliski does not disclose that a "portion of a shared secret" used to "scramble" or "unscramble" the "user terminal certificate" is disqualified from use "with symmetric key cryptography between the user terminal and the access point." Hind does not disclose this

15685.P207 FOA

- 12 -

Remarks

limitation either, and thus cannot cure the deficiency of Kaliski.

Accordingly, Applicants respectfully submit that independent claims 1, 7, 13, 18, 23, and 29 are in condition for allowance, as they recite limitations not disclosed by Kaliski or Hind. Furthermore, Applicants submit that dependent claims 2-3, 8-9, and 24-25 necessarily include the limitations of the independent claims from which they depend, and therefore also recite limitations not disclosed by Kaliski or Hind. For the reasons discussed above, Applicants respectfully request the PTO withdraw its rejection to claims 1-3, 7-9, 13, 18, 23-25, and 29.

**Claims 4, 10, 14, 19, 26, and 30 rejected under 35 U.S.C. § 103(a)**

Claims 4, 10, 14, 19, 26, and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaliski, in view of Hind, and in further view of US patent 6,754,824 to Persson, et al. ("Persson").

As discussed above with reference to independent claims 1, 7, 13, 18, 23, and 29, neither Kaliski nor Hind disclose that a "portion of a shared secret" used to "scramble" or "unscramble" the "user terminal certificate" is disqualified from use "with symmetric key cryptography between the user terminal and the access point," as claimed by Applicants. Similarly, Persson also fails to disclose this limitation, and thus cannot cure the deficiency of Kaliski and Hind. Dependent claims 4, 10, 14, 19, 26, and 30 necessarily include the limitations of the independent claims from which they depend, and therefore also recite limitations not disclosed by Kaliski, or Hind, or Persson.

Accordingly, Applicants respectfully submit that dependent claims 4, 10, 14, 19, 26, and 30 are in condition for allowance. For these reasons, Applicants respectfully request the PTO withdraw its rejection to claims 4, 10, 14, 19, 26, and 30.

15685.P207 FOA

- 13 -

Remarks

**New Claims 34-42**

New independent claim 34 presented herein recites:

An apparatus comprising:

a memory to store a certificate;

a processor coupled to the memory to scramble the certificate using a first portion of a shared secret to be known only by the apparatus and an access point of a wireless access network, wherein the first portion of the shared secret to be disqualified from use with symmetric key cryptography with the access point; and

a transmitter coupled to the processor to send a message to the access point, the message including the scrambled certificate.

New independent claim 39 presented herein recites a similar limitation to "unscramble the certificate" instead of "scramble the certificate." As discussed above with reference to independent claims 1, 7, 13, 18, 23, and 29, neither Kaliski, Hind, nor Persson disclose the limitations wherein a "portion of a shared secret" used to "scramble" or "unscramble" the "certificate" is disqualified from use "with symmetric key cryptography with the access point," as claimed by Applicants.

Accordingly, Applicants respectfully submit that new independent claims 34 and 39 as presented herein are in condition for allowance as they recite limitations not disclosed by Kaliski, Hind, or Persson. Furthermore, Applicants assert that new dependent claims 35-38 and 39-42 are also in condition for allowance as they necessarily incorporate the limitations from the independent claims upon which they depend. For these reasons, Applicants respectfully request the PTO allow new claims 34-42 as presented herein.

RECEIVED  
CENTRAL FAX CENTER

JAN 16 2007

**Conclusion**


Given the above amendments and accompanying remarks, all claims pending in the application are in condition for allowance. If the undersigned attorney has overlooked subject matter in any of the cited references that is relevant to allowance of the claims, the Examiner is requested to specifically point out where such subject matter may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (503) 439-8778.

**Charge Deposit Account**

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR &amp; ZAFMAN LLP

Date: 1-16-07  
\_\_\_\_\_  
Alan K. Aldous  
Attorney for Applicants  
Registration No. 31,905

Blakely, Sokoloff, Taylor & Zafman LLP  
12400 Wilshire Boulevard, Seventh Floor  
Los Angeles CA 90025-1030  
Phone: (503) 439-8778  
Facsimile: (503) 439-6073